UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,378	01/09/2004	Bindu Rama Rao	14316US02	7763

23446 7590 07/13/2009
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
AGWUMEZIE, CHARLES C	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
07/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/754,378	**Applicant(s)** RAO ET AL.	
	Examiner CHARLES C. AGWUMEZIE	**Art Unit** 3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-2 and 4-40* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *05/10/04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Acknowledgments

1. Applicant's amendment filed on May 1, 2009 is acknowledged. Accordingly claims 1-2, and 4-40 remain pending.

Response to Arguments

2. Applicant's arguments filed May 1, 2009 with respect to claim 1-2, and 4-19 have been fully considered but they are not persuasive.

3. With respect to **claim 1**, Applicant argues that the cited combination does not teach, suggest, or otherwise render obvious the subject matter claimed by claim 1; that the office action does not present a prima facie case of obviousness for claim 1 or its dependent claims.

In response, Examiner respectfully disagrees and submits that applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both references are concerned with updating software in a device. Though Hayes did not mention notification history server, Hayes did however describe all the functions of the notification history server and Naito was only used for the purpose of disclosing the keyword of notification history server. Furthermore, the Examiner notes that KSR forecloses the argument that a specific teaching, suggestion, or motivation is required to support a finding of obviousness. See *KSR*, 127 S. Ct. at 1741, 82 USPQ2d at 1396.

4. Applicant further argues that Hayes does not teach, suggest or otherwise render obvious "determining the authenticity of the notification in the electronic device, wherein determining the authenticity of the notification comprises contacting a notification history server, the notification history server keeping a record of notifications sent to the electronic device."

In response, Examiner respectfully disagrees and submits that Hayes does disclose or suggest or otherwise render obvious "determining the authenticity of the notification in the electronic device, wherein determining the authenticity of the notification comprises contacting a notification history server, the notification history server keeping a record of notifications sent to the electronic device." Hayes made it clear that the wireless programmer 200 (notification history server) continuously transmits a plurality of sequential notification frames N.sub.i 456, each of which may carry unique update notification data. .... notification frame N1 may carry notification information for updating a first model of cellular telephones to a first revision level, while notification frame N2 carries notification information for updating a second model of cellular telephones to a second revision level, and so forth…(see col. 9, line 55-col. 10, line 2). Hayes further made it clear that upon the receipt of the notification frames from the wireless programmer 200, an authentication takes places between the wireless programmer and the devices in order to ensure that the notification is from the wireless programmer 200 (see fig. 5A). The purpose of the authentication is to ensure the authenticity of the notification sent from the wireless programmer. Also notice that the wireless programmer keeps the record of the notification sent and to which devices they were sent to. This is the only way the wireless programmer is able to know which devices that have responded to the notifications. Accordingly it is Examiner's position that Hayes does disclose the claimed limitation. Naito is used only for the purpose of using the keyword notification server.

5. Applicant further argues that the authentication of two devices is quite different from and does not teach, determining the authenticity of the notification as claimed. That the authentication disclosed in Hayes is merely the authentication of the devices that sends the notification of Hayes and not the authentication of a notification.

In response, Examiner respectfully disagrees with Applicant's characterization and submits that the authentication of the devices in Hayes is predicated upon verifying and/or authenticating the sent notification from the wireless programmer 200 (notification history server) to the devices. Accordingly it is Examiner's position that Hayes does disclose the claimed limitation.

6. Applicant further argues that Hayes is also silent with respect to determining the authenticity of the notification in the electronic device, wherein determining the authenticity of the notification comprises contacting a notification history server as claimed. Further, Applicants also respectfully submit that this portion of Hayes similarly fails to teach, suggest, or otherwise render obvious "the notification history server keeping a record of notifications sent to the electronic device" as claimed.

In response, Examiner respectfully disagrees with Applicant's characterization and incorporates by reference the preceding discussions as if fully re-written herein. Hayes made it clear that upon receipt of the notification sent the wireless programmer 200, an authentication (contacting the wireless programmer 200 by the phone) takes places (see fig. 5A). Thus Hayes does disclose contacting the notification history server as claimed.

7. Applicant further argues that Hayes does not teach or suggest or otherwise render obvious "the notification history server keeping a record of notification sent to the electronic device" as claimed.

In response, Examiner respectfully disagrees and submits that Hayes does disclose "the notification history server keeping a record of notification sent to the electronic device" as claimed. If the wireless programmer does not keep record of the devices that notification was sent to, how then does the wireless programmer able to identify the devices which has responded to the notification. Not only does the wireless programmer keep record of the notifications sent to the devices but also keep the results of the authentication between the wireless programmer and devices which was predicated upon verifying that the notification is sent by the authorized wireless programmer.

8. Applicant further argues that updated software and revision number of the updated software as well as a list of electronic devices ...which have been successfully reprogrammed is different from the claimed subject matter which relates to determining the authenticity of the notification including contacting a notification history server that keeps a record of the notifications sent to the electronic device.

In response Examiner respectfully disagrees and submits that Hayes does disclose the claimed limitation. Hayes wireless programmer 200 keeps record of notifications sent to electronic devices including the authentication results. The argument that the record is kept after the update had already been performed is not the issue. The records are there even before the updates are performed because the authentication and the result of the authentication are performed before the update takes place. The fact that the record of the successfully update devices are later kept as well in order to identify those whose updates were successful and those that are not successful does not remove the fact that the records of the notification are kept by the wireless programmer. If the records are not there prior to update how then does the wireless programmer 200 know which machines are legitimate and which once are not?

With respect to **claim 13**, Applicant argues that claim 13 is dependent from claim 1 and therefore patentable over the cited combination of references.

In response, Examiner respectfully disagrees and submits that claim 13 is neither patentable being dependent from claim 1 nor for its individual recited features.

9. Applicant's arguments with respect to claims 20-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. **Claims 1-2, and 4-19**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hayes, Jr. et al (hereinafter "Hayes") U.S. Patent No. 5,974,312 in view of Naito et al (hereinafter "Naito") U.S. Patent Application Publication No. 2004/0153549 A1.

12. As per **claim 1**, Hayes, discloses a method of updating, the method comprising:

receiving a notification in the electronic device (see fig. 5A, which discloses notification to phone); and

determining the authenticity of the notification in the electronic device, wherein determining the authenticity of the notification comprises contacting a notification history server, the notification history server keeping a record of notifications sent to the electronic device (see fig. 5A, which discloses authentication of the notification by phone; col. 2, lines 35-50, the wireless programmer stores the updated software, revision number of the updated software, and (at the end of the re-programming process) a list of electronic devices by serial number which have been successfully re-programmed, and their corresponding software revision levels; col. 13, lines 55-60, which discloses that the wireless programmer 200 has been authenticated...; col. 15, lines 25-40).

13. What Hayes does not explicitly use is the claim term a notification history server. Hayes however discloses a notification channel for notifying the mobile devices of updates. A person of ordinary skill in the art would understand that wireless programmer 200 is equivalent to the claimed notification history server.

14. Alternatively Naito discloses a notification history server (0126)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Hayes and incorporate the method of contacting a notification history server in view of the teachings of Naito in order to ensure that signals from only legitimate servers are responded to and in addition the since the claimed invention is merely a combination of old and known elements and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

15. As per **claim 2,** Hayes further discloses the method, further comprising: informing the electronic device of availability of at least one update package for updating at least one of firmware and software resident in the electronic device (col. 9, lines 55-68); but failed to explicitly disclose

simultaneously informing a notification history server that a notification has been sent to the electronic device.

Naito discloses simultaneously informing a notification history server that a notification has been sent to the electronic device (0126)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Hayes and incorporate the method of simultaneously informing a notification history server that a notification has been sent to the electronic device in view of the teachings of Naito since the claimed invention is merely a combination of old and known elements and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

16. As per **claim 4**, Hayes further discloses the method, further comprising: ignoring the notification in the electronic device upon determining that the notification is inauthentic (col. 13, line 60-col. 14, line 5; col. 15, line 40-col. 16, line 5);

recording that an inauthentic notification has been received (col. 15, line 40-col. 16, line 5); and

waiting to receive another notification in the electronic device (col. 13, line 60-col. 14, line).

17. As per **claim 5**, Hayes further discloses the method, further comprising:

determining identification information of a server and update package associated with the notification upon determining that the notification received in the electronic device is authentic (col. 9, lines 40-68, which discloses channel identification code or unique update notification data…and revision number of the new software….).

18. As per **claim 6**, Hayes further discloses the method, further comprising:

retrieving the update package (see fig. 3; col. 3, lines 10-20); and

performing an update of at least one of firmware and software resident in the electronic device (col. 10, lines 10-40).

19. As per **claim 7**, Hayes further discloses the method, wherein the notification comprises one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification (see fig. 1).

20. As per **claim 8**, Hayes further discloses the method, wherein the electronic device comprises one of a mobile cellular phone handset, a personal digital assistant, a pager, an MP3 player, and a digital camera (see fig. 1).

21. As per **claim 9**, Hayes further discloses the method, wherein determining the authenticity of the notification in the electronic device further comprises determining whether the notification was sent from an authorized server (see fig. 5A, which discloses authentication between the wireless programmer and the phone).

22. As per **claim 10**, Hayes further discloses the method, wherein an authorized server comprises one of a management server and a customer care center (col. 12, lines 35-45, which discloses under the control of an operator).

23. As per **claim 11**, Hayes further discloses the method, wherein the notification comprises location and identification information regarding a management server providing access to an update package and information regarding the update package (col. 9, lines 40-68, which discloses channel identification code or unique update notification data...and revision number of the new software....).

24. As per **claim 12**, Hayes further discloses the method, wherein location and identification information comprise at least one of a universal resource locator (URL), an internet protocol (IP) address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information (col. 9, lines 40-68, which discloses unique update notification data...).

25. As per **claim 14**, Hayes further discloses the method, wherein retrieving the update package from the default management server is performed after authentication of the notification message (see fig. 5A, which discloses authentication).

26. As per **claim 15**, Hayes further discloses the method, further comprising:

retrieving an update package via a download agent in the electronic device (see fig. 1, mobile phone has software that enables it to retrieve or download firmware and other updates); and

updating at least one of firmware and software in the electronic device via an update agent in the electronic device (see fig. 5F which discloses successful update…).

27. As per **claim 16**, Hayes further discloses the method, further comprising preventing unauthorized updates of at least one of firmware and software in the electronic device (see fig. 8A, which discloses turn phone off if the number of attempts to authenticate is exceeded).

28. As per **claim 17**, Hayes further discloses the method, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process, and when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic (see fig. 8A).

29. As per **claim 18**, Hayes further discloses the method, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device (col. 12, lines 1-20, which discloses "a key");

accessing a static key component from memory in the electronic device (col. 12, lines 1-20, which discloses ESN); and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package (col. 12, lines 20-35).

30. As per **claim 19**, Hayes further discloses the method, further comprising provisioning an address of a management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event (col. 14, lines 40-65).

31. **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over Hayes, Jr. et al (hereinafter "Hayes") U.S. Patent No. 5,974,312 in view of Naito et al (hereinafter "Naito") U.S. Patent Application Publication No. 2004/0153549 A1 as applied to claim 1 above, and further in view of Marsh et al (hereinafter "Marsh") U.S. Patent Application Publication No. 2002/0073304 A1.

32. As per **claim 13**, Hayes failed to explicitly disclose the method, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event.

Marsh discloses the method, further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event (0013; 0014; 0015).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Hayes and incorporate the method further comprising retrieving an update package from a default management server by accessing an address of the default management server when no server address information is included in the notification, the address of the default management server being provisioned in the electronic device during a bootstrap provisioning event in view of the teachings of Marsh in order to ensure that notification is sent only by legitimate servers and in addition since the claimed invention is merely a combination of old and known elements and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

33. **Claims 20-22 and 24-38**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Sadwosky U.S. Patent No. 6,123,737.

34. As per **claim 20**, Sadowsky discloses a mobile services network at least comprising:

at least one electronic device (see fig. 1; client computer);

a management server communicatively linked with the at least one electronic device via a communication link (fig. 1; server 2(1)-2(n)); and

a notification history server (fig. 2, email system 19) operatively connected to the management server (fig. 1; server 2(1)-2(n), the notification history server comprising a record of authentic notifications sent to the at least one electronic device (fig. 1; the server computer 2 generates a notification package 12, 13, 14, sent over the a communication interface);

wherein the electronic device is adapted to determine the authenticity of the notifications by contacting the notification history server (see figs. 3, which discloses authentic and valid 64).

What Sadwosky does not explicitly use is the claim term management server. However a person of ordinary skill in the art would recognize that any of the servers 2(1) -2(n) could serve as the management server. Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky by substituting any of the servers 2(1)-2(n) with the management server.

35. As per **claim 21**, Sadowsky further discloses the network, wherein the electronic device at least comprises:

non-volatile memory (fig. 1, client computer);

a short message entity; random access memory; and security services (fig. 1).

36. As per **claim 22**, Sadowsky further discloses the network, wherein the non-volatile memory in the electronic device at least stores:

an update agent (fig. 1);

a firmware and real-time operating system (fig. 1; col. 3, lines 5-20);

an operating system layer (fig. 1; col. 3, lines 5-20);

a download agent or browser (fig. 1); and

an end-user related data and content (see abstract; software package 18).

37. As per **claim 24**, Sadowsky further discloses the network, wherein the electronic device is adapted to receive notifications informing the electronic device of availability of update packages at the management server (see figs. 3).

38. As per **claim 25,** Sadwosky further discloses the network wherein the notification history server is adapted to determine whether a notification is authentic by examining message identification information in the notifications (see fig. 3 and 4).

39. As per **claim 26**, Sadwosky further discloses the network, wherein the electronic device is adapted to download an update package from an update package repository using an update agent upon determining that a notification received in the electronic device is authentic (see figs. 3 and 4; col. 4, lines 45-50).

40. As per **claim 27**, Sadwosky further discloses the network, wherein the electronic device is adapted to determine whether a notification originated from an authorized sender (col. 4, lines 45-50).

41. As per **claim 28**, Sadwosky further discloses the network, wherein an authorized sender is at least one of the management server and a customer care center resident in the network (fig. 3).

42. As per **claim 29,** Sadwosky further discloses the network, further comprising a short message center (SMC) adapted to store and forward messages to and from the electronic device, wherein the short message center (SMC) is adapted to send, upon instruction from the management server or a customer care center, notifications to the electronic device regarding availability of update packages (col. 2, lines 30-35, 60-65).

43. As per **claim 30**, Sadwosky further discloses the network, wherein notifications comprise at least one of a short message service (SMS) notification, an instant messaging (IM) notification, an email notification, a wireless application protocol (WAP) push message notification, and an enhanced messaging service (EMS) notification (see figs. 3, 4 and 5).

44. As per **claim 31**, Sadwosky further discloses the network, wherein notifications further comprise at least one user data field containing message identification information (fig. 5; col. 5, lines 50-65).

45. As per **claim 32**, Sadwosky further discloses the network, wherein notifications further comprise location and identification information regarding a management server providing access to an update package and information regarding the update package (col. 5, line 50-col. 6, line 15; col. 6, line 30-35).

46. As per **claim 33**, Sadwosky further discloses the network, wherein location and identification information comprise at least one of a universal resource locator, an internet protocol address, a dynamic security key, end-user data, program update information, download scheduling information, and notification protocol information (col. 6, line 30-35).

47. As per **claim 34**, Sadwosky further discloses the network, wherein upon determining that a notification received in the electronic device is inauthentic, the electronic device is adapted to ignore the notification and wait for another notification, and a record is created recording that an inauthentic notification has been received (col. 4, lines 40-50).

48. As per **claim 35**, Sadwosky further discloses the network, wherein the management server comprises the notification history server and an update package repository (fig. 3).

49. As per **claim 36**, Sadwosky further discloses the network, wherein the notification history server is incorporated into a short message center in the network (see fig. 3).

50. As per **claim 37**, Sadwosky further discloses the network, further comprising a security service in the electronic device for preventing unauthorized updating of at least one of firmware and software in the electronic device (col. 4, lines 40-50).

51. As per **claim 38**, Sadwosky further discloses the network, wherein preventing unauthorized updates further comprises:

when a notification sent to the electronic device is discernable by an end-user and the end-user is prompted to initiate an update process (col. 5, line 50-65), and

when the end-user initiates the update process, the electronic device is adapted to determine the authenticity of the notification, and abort the update process if the notification is determined to be inauthentic, and permit the update package to be downloaded, if the notification is determined to be authentic (col. 4, lines 40-50).

52. **Claims 23 and 39-40**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Sadwosky U.S. Patent No. 6,123,737 in view of Hayes, Jr. et al (hereinafter "Hayes") U.S. Patent No. 5,974,312.

53. As per **claim 23**, Sadwosky failed to explicitly disclose the network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera.

Hayes discloses the network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera (fig. 1).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the network comprising network, wherein the electronic device comprises one of a mobile cellular phone handset, personal digital assistant, pager, MP3 player, and a digital camera in view of the teachings of Hayes in order to identify the equipment employed.

54. As per **claim 39**, Sadwosky failed to explicitly disclose the network, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device;

accessing a static key component from memory in the electronic device; and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package.

Hayes discloses the network, wherein preventing unauthorized updates further comprises:

receiving a dynamic key component from a management server in the electronic device (col. 12, lines 1-20, which discloses “a key”);

accessing a static key component from memory in the electronic device (col. 12, lines 20-35); and

instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package (col. 12, lines 20-35).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant’s invention to modify the method of Sadwosky and incorporate the network comprising receiving a dynamic key component from a management server in the electronic device; accessing a static key component from memory in the electronic device; and instructing a download agent to use the dynamic key component and the static key component to generate a security key, wherein the generated security key facilitates access to a downloadable update package in an update package repository if the electronic device is authorized access to the update package, otherwise the electronic device is denied access to the update package in view of the teachings of Hayes in order to ensure security.

55. As per **claim 40,** Sadwosky failed to explicitly disclose the network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event.

Hayes discloses a the network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event (col. 14, lines 40-65)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Sadwosky and incorporate the network comprising network, wherein the network is adapted to provision the address of the management server in the electronic device during a bootstrap provisioning event by sending a notification, the notification comprising server address information, and wherein the electronic device is adapted to access and employ the address of the management server provisioned in the electronic device after the bootstrap provisioning event in view of the teachings of Hayes in order to ensure security.

Conclusion

56. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin Hewitt can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
July 8, 2009